

## UNITED STATES DISTRICT COURT

for the  
Southern District of OhioIn the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)PNY SD card and PNY Premium SD card, currently  
located at the Federal Bureau of Investigation, 7747 Cloyo  
Road, Centerville, Ohio, 45459

Case No.

3:15mj-525

MICHAEL J. NEWMAN

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under  
penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the  
property to be searched and give its location):  
See Attachment Alocated in the Southern District of Ohio, there is now concealed (identify the  
person or describe the property to be seized):  
See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

See Attachment C

Offense Description

The application is based on these facts:  
See Attached Affidavit

- ☐ Continued on the attached sheet.
- ☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested  
under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Andrea R. Kinzig

Applicant's signature

Andrea R. Kinzig, Special Agent

Printed name and title

Sworn to before me and signed in my presence.

Date:

12/3/15

City and state: Dayton, Ohio



Judge's signature

Michael J. Newman, U.S. Magistrate Judge

Printed name and title

FILED  
RICHARD W. MAGEL  
CLERK OF COURT  
2015 DEC -3 PM 3:39  
U.S. DISTRICT COURT  
SOUTHERN DIST. OHIO  
WESTERN DIV. DAYTON

**ATTACHMENT A**

PNY SD card and PNY Premium SD card ("Subject Devices"), which were obtained from the residence located at 217 Prentice Drive, New Carlisle, Ohio, 45344. The Subject Devices are currently located at the Federal Bureau of Investigation, 7747 Clys Road, Centerville, Ohio, 45459.

**ATTACHMENT B**  
**Particular Things to be Seized**

1. Any visual depictions and records related to the possession, receipt, and distribution of child pornography;
2. Any visual depictions of minors and any associated EXIF data and file property information;
3. Any communications with others in which child exploitation materials and offenses are discussed and/or traded, and any contact / identifying information for these individuals;
4. Any communications with minors, and any contact / identifying information for these minors;
5. Evidence of utilization of email accounts, social media accounts, online chat programs, file storage accounts, including any account / user names;
6. Any information regarding utilization of websites and social media sites to access or obtain child pornography, communicate with juveniles, or communicate with others regarding child exploitation offenses;
7. Evidence of utilization of aliases and fictitious names;
8. Information relating to who used the Subject Devices, including records about their identities and whereabouts.

**ATTACHMENT C**

<u>Code Section</u>	<u>Offense Description</u>
18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2)	Possession of Child Pornography
18 U.S.C. §2252(a)(4)(B) & (b)(2)	Possession of Child Pornography
18 U.S.C. §2252(a)(2)(B) & (b)(1)	Distribution and Receipt of Child Pornography
18 U.S.C. §2252A(a)(2)(A) and (b)(1)	Distribution and Receipt of Child Pornography
18 U.S.C. §2251(a) & (e)	Production of Child Pornography
18 U.S.C. §2422(b)	Coercion and Enticement



**AFFIDAVIT IN SUPPORT OF SEARCH WARRANT**

I, Andrea R. Kinzig, being duly sworn, depose and state the following:

**INTRODUCTION**

1. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI), and have been so employed since 2005. I am currently assigned to the Dayton, Ohio Resident Agency of the Cincinnati Field Office. In connection with my official duties, I investigate violations of federal criminal laws, including offenses pertaining to the illegal production, distribution, receipt, and possession of child pornography (in violation of 18 U.S.C. §§ 2252(a), 2252A, and 2251) and offenses pertaining to coercion and enticement (in violation of 18 U.S.C. § 2422(b)). I have received training in the area of child pornography and child exploitation and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in various forms of media including computer media.
2. Along with other agents and officers of the Federal Bureau of Investigation and Clark County (Ohio) Sheriff's Office, I am currently involved in an investigation of the possession, distribution, receipt, and production of child pornography and coercion and enticement by JAMES EDWARD RISNER III (hereinafter referred to as JAMES RISNER). This Affidavit is submitted in support of an Application for a search warrant for the following:
  - a. PNY SD card and PNY Premium SD card, currently located at the Federal Bureau of Investigation, 7747 Cloyo Road, Centerville, Ohio, 45459 (hereinafter referred to as "**Subject Devices**").
3. The **Subject Devices** are more fully described in Attachment A. The purpose of the Application is to seize evidence of violations of 18 U.S.C. §§ 2252(a)(4)(B) and 2252A(a)(5)(B), which make it a crime to possess child pornography; violations of 18 U.S.C. §§ 2252(a)(2) and 2252A(a)(2), which make it a crime to receive and distribute child pornography through interstate commerce; violations of 18 U.S.C. §§ 2251(a) and (e), which make it a crime to produce child pornography; and violations of 18 U.S.C. § 2422(b), which make it a crime to use a facility of interstate commerce to coerce and entice another individual to engage in illegal sexual activities. The items to be searched for and seized are described more particularly in Attachment B.
4. As part of the investigation, I have reviewed documentation and reports provided by and discussed information with other officers involved in the investigation. For purposes of this Affidavit, I have not distinguished between information of which I have direct knowledge and that of which I have hearsay knowledge.
5. This Affidavit does not contain every fact known to the investigation, but only those deemed necessary to demonstrate sufficient probable cause to support searches of the **Subject Devices** (as described in Attachment A).

6. As a result of the instant investigation described more fully below, there is probable cause to believe that evidence, fruits, and instrumentalities of violations of federal law, including 18 U.S.C. §§ 2251, 2252, 2252A, and 2422, are present within the information associated with the **Subject Devices** (as described in Attachment A).

### **BACKGROUND INFORMATION**

#### Pertinent Federal Statutes

7. 18 U.S.C. § 2252(a)(4)(B) states that it is a violation for any person to knowingly possess, or knowingly possess with the intent to view, one or more matters which contain any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer if the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.
8. 18 U.S.C. § 2252A(a)(5)(B) states that it is a violation for any person to knowingly possess, or knowingly access with intent to view, any book, magazine, periodical, film, videotape, computer, disk, or any other material that contains an image of child pornography that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, that was produced using materials that have been mailed, or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.
9. 18 U.S.C. § 2252(a)(2)(B) states that it is a violation for any person to knowingly receive or distribute any visual depiction using any means or facility of interstate or foreign commerce or that has been mailed, shipped, or transported in or affecting interstate or foreign commerce or which contains materials which have been mailed or so shipped or transported by any means, including by computer, or to knowingly reproduce any visual depiction for distribution using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or through the mails if the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.
10. 18 U.S.C. § 2252A(a)(2) states that it is a violation for any person to receive or distribute – (A) any child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer; and (B) any material that contains child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.
11. 18 U.S.C. §§ 2251(a) and (e) states that it is a violation for any person to knowingly employ, use, persuade, induce, entice, or coerce any minor to engage in, or to have a minor assist any other person to engage in, or to transport any minor in or affecting



interstate or foreign commerce, or in any Territory or Possession of the United States, with the intent that such minor engage in any sexually explicit conduct for the purpose of producing any visual depiction of such conduct or for the purpose of transmitting a live visual depiction of such conduct, when he knew or had reason to know that such visual depiction would be transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed, if that visual depiction was produced or transmitted using materials that have been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer, or if such visual depiction has actually been transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed, or attempts or conspires to do so.

12. For purposes of these statutes, the term “sexually explicit conduct” is defined in 18 U.S.C. § 2256(2) as:

a. “Actual or simulated –

- i. Sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex;
- ii. Bestiality;
- iii. Masturbation;
- iv. Sadistic or masochistic abuse; or
- v. Lascivious exhibition of genitals or pubic area of any person.”

13. 18 U.S.C. § 2422(b) states that is a violation for any person to use the mail or any facility or means of interstate or foreign commerce, or within the special maritime and territorial jurisdiction of the United States, to knowingly persuade, induce, entice, or coerce any individual who has not attained the age of 18 years, to engage in prostitution or any sexual activity for which any person can be charged with a criminal offense, or attempt to do so.

#### Definitions

14. The following definitions apply to this Affidavit and Attachment B to this Affidavit:

- a. “**Child Pornography**” includes the definition in Title 18 U.S.C. § 2256(8) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct).
- b. “**Visual depictions**” include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image (see 18 U.S.C. § 2256(5)).

- c. “**Minor**” means any person under the age of eighteen years (see 18 U.S.C. § 2256(1)).
- d. “**Sexually explicit conduct**” means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person (see 18 U.S.C. § 2256(2)).
- e. “**Internet Service Providers**” or “**ISPs**” are commercial organizations which provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers, including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer various means by which to access the Internet including telephone based dial-up, broadband based access via a digital subscriber line (DSL) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth that the connection supports. Many ISPs assign each subscriber an account name such as a user name or screen name, an e-mail address, and an e-mail mailbox, and the subscriber typically creates a password for the account. By using a computer equipped with a telephone or cable modem, the subscriber can establish communication with an ISP over a telephone line or through a cable system, and can access the Internet by using his or her account name and password.
- f. An **Internet Protocol address**, also referred to as an **IP address**, is a unique numeric address that computers or electronic devices use in order to communicate with each other on a computer network utilizing the Internet Protocol (IP) standard. Every computer or device connected to the Internet is referenced by a unique IP address. An IP address can be thought of as the equivalent to a street address or a phone number, just as each street address and phone number uniquely identifies a building or telephone. IP addresses are composed of four sets of digits known as “octets,” ranging in value from 0-255, separated by decimal points. An example of an IP address is 192.168.10.102. There are two types of IP addresses; static and dynamic. A static address is permanently assigned to a particular device and as a practical matter never changes. A dynamic address provided by an Internet service provider to a client computer is valid only for the duration of the session that the client computer is connected to the Internet (or other network).
- g. A network “**server**,” also referred to as a “**host**,” is a computer system that has been designated to run a specific server application or applications and provide requested services to a “client” computer. A server can be configured to provide a wide variety of services over a network, including functioning as a web server, mail server, database server, backup server, print server, FTP (File Transfer Protocol) server, DNS (Domain Name System) server, to name just a few.
- h. A **client** is the counterpart of a server or host. A client is a computer system that accesses a remote service on another computer by some kind of network. Web browsers (like Internet Explorer or Safari) are clients that connect to web servers and



- retrieve web pages for display. E-mail clients (like Microsoft Outlook or Eudora) retrieve their e-mail from their Internet service provider's mail storage servers.
- i. **“Domain Name”** refers to the common, easy to remember names associated with an Internet Protocol address. For example, a domain name of “www.usdoj.gov” refers to the Internet Protocol address of 149.101.1.32. Domain names are typically strings of alphanumeric characters, with each level delimited by a period. Each level, read backwards – from right to left – further identifies parts of an organization. Examples of first level, or top level domains are typically “.com” for commercial organizations, “.gov” for the governmental organizations, “.org” for organizations, and, “.edu” for educational organizations. Second level names will further identify the organization, for example “usdoj.gov” further identifies the United States governmental agency to be the Department of Justice. Additional levels may exist as needed until each machine is uniquely identifiable. For example, www.usdoj.gov identifies the World Wide Web server located at the United States Department of Justice, which is part of the United States government. The Domain Name System, also referred to DNS, is a system of servers connected to each other using a common system of databases that resolve a particular domain name, such as “www.usdoj.gov,” to its currently assigned IP address (*i.e.*, 149.101.1.32), to enable the follow of traffic across the Internet.
  - j. **“Log Files”** are records automatically produced by computer programs to document electronic events that occur on computers. Computer programs can record a wide range of events including remote access, file transfers, logon/logoff times, and system errors. Logs are often named based on the types of information they contain. For example, web logs contain specific information about when a website was accessed by remote computers; access logs list specific information about when a computer was accessed from a remote location; and file transfer logs list detailed information concerning files that are remotely transferred.
  - k. **“Hyperlink”** (often referred to simply as a “link”) refers to a navigation element in a web page or document that automatically brings the referred information (a.k.a. “resource”) to the user when the navigation element is selected by the user. Hyperlinks are part of the foundation of the World Wide Web, but are not limited to a website for HTML.
  - l. **“Website”** consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).
  - m. **“Uniform Resource Locator”** or **“Universal Resource Locator”** or **“URL”** is the unique address for a file that is accessible on the Internet. For example, a common way to get to a website is to enter the URL of the website’s home page file in the Web browser’s address line. Additionally, any file within that website can be specified with a URL. The URL contains the name of the protocol to be used to access the file resource, a domain name that identifies a specific computer on the Internet, and a pathname, a hierarchical description that specifies the location of a file in that computer.

- n. The terms “**records**,” “**documents**,” and “**materials**,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

#### Characteristics of Collectors of Child Pornography

15. Based upon my knowledge, experience, and training in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved in the collection of child pornography (hereafter “collectors”):
- a. Collectors may receive sexual stimulation and satisfaction from contact with children, or from having fantasies of children engaged in sexual activity or suggestive poses, or from literature describing such activity.
  - b. Collectors may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Collectors typically use these materials for their own sexual arousal and gratification. Collectors often have companion collections of child erotica. Child erotica are materials or items that are sexually suggestive and arousing to pedophiles, but which are not in and of themselves obscene or pornographic. Such items may include photographs of clothed children, drawings, sketches, fantasy writings, diaries, pedophilic literature and sexual aids.
  - c. Collectors who also actively seek to engage in sexual activity with children may use these materials to lower the inhibitions of a child they are attempting to seduce, convince the child of the normalcy of such conduct, sexually arouse their selected child partner, or demonstrate how to perform the desired sexual acts.
  - d. Collectors almost always possess and maintain their “hard copies” of child pornographic images and reference materials (*e.g.*, mailing and address lists) in a private and secure location. With the growth of the Internet and computers, a large percentage of most collections today are in digital format. Typically these materials are kept at the collector’s residence for easy access and viewing. Collectors usually place high value on their materials because of the difficulty, and legal and social danger, associated with acquiring them. As a result, it is not uncommon for collectors to retain child pornography for long periods of time, even for years. Collectors often



- discard child pornography images only while “culling” their collections to improve their overall quality.
- e. Collectors also may correspond with and/or meet others to share information and materials. They may save correspondence from other child pornography distributors/collectors, including contact information like email addresses, and may conceal such correspondence as they do their sexually explicit material.
  - f. Collectors prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.
  - g. Subscribers to websites that are primarily designed to provide child pornography have a strong likelihood of being collectors of child pornography. This high degree of correlation between subscription and collection behavior has been repeatedly confirmed during several recent nationwide law enforcement initiatives, including ICE’s “Operation Emissary” and the FBI’s “Ranchi message board” investigation. For example, in the “Ranchi” investigation a national take-down occurred during the week of March 1, 2007. Approximately 83 subjects were contacted, 28 by court-authorized search warrants and 55 by “knock and talks.” Of the 83 contacts, 46 individuals (or 55%) confessed to accessing the Ranchi message board and/or downloading child pornography from Ranchi. Multiple other new cases were opened without confessions based on strong evidence obtained during the Ranchi search warrants and knock-and-talks.

#### Use of Computers with Child Pornography

16. Computers and computer technology have revolutionized the way in which child pornography is produced, distributed, and utilized. It has also revolutionized the way in which child pornography collectors interact with each other, as well the methods that individuals will use to interact with and sexually exploit children. Computers serve four functions in connection with child pornography: production; communication; distribution and storage.
- a. **Production:** Pornographers can now produce both still and moving images directly from a common video camera. The camera is attached, using a cable, directly to the computer using a device called a video capture board. This device turns the video output into a form that is usable by computer programs. The output of the video camera can be stored, manipulated, transferred or printed directly from the computer. The captured image can be edited (*i.e.*, lightened, darkened, cropped, digitally enhanced, *etc.*) with a variety of commonly available graphics programs. The producers of child pornography can also use scanners to convert hard-copy photographs into digital images.
  - b. **Communication.** Previously, child pornography collectors had to rely on personal contact, U.S. mail, and telephonic communications in order to sell, trade, or market pornography. Today most communications associated with the trafficking of child pornography occur via the obscurity and relative anonymity of the Internet. A device

known as a modem allows any computer to connect to the Internet via telephone lines or broadband Internet connections. Once connected to the Internet, individuals search for and/or offer to distribute child pornography in a wide variety of ways. Many individuals congregate in topic-based Internet chat rooms implicitly or explicitly dedicated to child pornography. Online discussions in these chat rooms are usually done via instant message (or "IM"), and individuals may then establish one-on-one chat sessions involving private messages (or "PMs"), visible only to the two parties, to trade child pornography. These child pornography images may be sent as attachments to the PMs, or they may be sent separately via electronic mail between the two parties. Pedophile websites communicate advertisements for the sale of child pornography, and individuals may order child pornography from these websites using email or send order information from their web browser (using HTTP computer language). Some individuals communicate via Internet Relay Chat (IRC) to discuss and trade child pornography images. It is not uncommon for child pornography collectors to engage in mutual validation of their interest in such material through Internet-based communications.

- c. **Distribution.** Computers and the Internet are the preferred method to distribute child pornography. As discussed above, such images may be distributed via electronic mail (either as an attachment or embedded image), or through instant messages as attachments. Child pornography is regularly downloaded from servers or Usenet newsgroups via a method known as FTP (file transfer protocol). Child pornography images are also distributed from websites via client computers web browsers downloading such images via HTTP (Hyper Text Transfer Protocol). Peer-to-peer networks such as LimeWire and Gnutella are an increasingly popular method by which child pornography images are distributed over the Internet.
- d. **Storage.** The computer's capability to store images in digital form makes it an ideal repository for pornography. A single floppy disk can store dozens of images and hundreds of pages of text. The size of computer hard drives used in home computers has grown tremendously within the last several years. Hard drives with the capacity of two hundred (200) gigabytes are not uncommon. These drives can store thousands of images at very high resolution. Remote storage of these images on servers physically removed from a collector's home computer adds another dimension to the equation. It is possible to use a video camera to capture an image, process that image in a computer with a video capture board, and save that image to storage in another country. Once this is done, there is no readily apparent evidence at the scene of the crime. Only with careful laboratory examination of electronic storage devices is it possible to recreate the evidence trail.

### **FACTS SUPPORTING PROBABLE CAUSE**

#### **Background of Investigation**

- 17. In November 2015, an undercover task force officer of the FBI (hereinafter referred to as UCO-1), operating in the Washington, D.C. area, conducted an online investigation of



individuals utilizing a file-sharing website to possess and distribute child pornography. This website will be referred to for purposes of this Affidavit as "Website A".

18. On or around November 23, 2015, UCO-1 located an account for an individual on Website A that had an album entitled "gymnastics daughter" and the following caption in the user profile: "email me for trade". The email address of [reset1800@gmail.com](mailto:reset1800@gmail.com) was also listed on the profile page. The album contained various pictures of a pre-pubescent white female child with blonde hair wearing a gymnastics leotard. An adult white male was depicted in one of the photographs, although only the lower portion of his face was captured. The adult male was wearing a t-shirt with a logo for the Cincinnati Bengals (a football team in Cincinnati, Ohio).
19. Also on or around November 23, 2015, UCO-1 sent an email message to [reset1800@gmail.com](mailto:reset1800@gmail.com) in which he identified himself as a "perv dad". The user of this email account quickly responded to UCO-1's message by stating "hi ok no prob s2r your dau pics only :)". Based on my training and experience, I know that "s2r" is a term to refer to "send to receive" and "dau" is short for "daughter". In my experience, I know that individuals involved in trading child pornography often request a new trading partner to send child pornography first to ensure that the new trading partner has files to share as well as to ensure that the new trading partner is not a law enforcement officer.
20. The [reset1800@gmail.com](mailto:reset1800@gmail.com) account user continued to exchange messages with UCO-1 from approximately November 23, 2015 to November 26, 2015. Below is a summary of these messages:
  - a. The [reset1800@gmail.com](mailto:reset1800@gmail.com) account user identified that the female child depicted in the photographs contained in the "gymnastics daughter" album was his daughter. The [reset1800@gmail.com](mailto:reset1800@gmail.com) account user stated that his daughter was five years old at the time of the photographs but was currently seven years old.
  - b. In the exchange of messages, the [reset1800@gmail.com](mailto:reset1800@gmail.com) account user asked UCO-1 if he was sexually active with his daughter. UCO-1 responded that he was, and the [reset1800@gmail.com](mailto:reset1800@gmail.com) account user then stated: "yup same all the way round w/pics just don't have any of me doing her but i have. I already stole that cherry". Later in the exchange of messages, the [reset1800@gmail.com](mailto:reset1800@gmail.com) account user stated: "Had to wait till she hit 7 to take her cherry to prevent tearing her and giving us away." Based on my training and experience, I believe that the [reset1800@gmail.com](mailto:reset1800@gmail.com) account user was telling UCO-1 that he had vaginal sexual intercourse with his daughter on previous occasions but had not taken pictures of the sexual intercourse.
  - c. Also in the exchange of messages, the [reset1800@gmail.com](mailto:reset1800@gmail.com) account user sent UCO-1 various links to images on Yandex, a Russian website. The links contained at least approximately twenty-six unique images of a pre-pubescent white female child that the [reset1800@gmail.com](mailto:reset1800@gmail.com) account user indicated or specifically identified was his daughter. The images depict close-up images of the child's groin area and buttocks, some of which depict the child wearing white underwear and some of which depict her nude vagina and/or buttocks. None of the images depict the child's face. In some of the images, the child's finger(s) is (are) inserted in her vagina or spreading apart her vagina. Based on my training and experience, I believe that at least

- approximately nineteen of the images depict child pornography (as defined by 18 U.S.C. § 2256).
- d. In two of the images noted above, the child had a piece of paper in her hand with UCO-1's undercover name and the date of the email message (November 24, 2015). These images were sent in response to an inquiry made by UCO-1 if the reset1800@gmail.com account user actually had access to children. Based on my training and experience, I know that individuals involved in producing and trading child pornography sometimes include such papers in their images and videos as a means to validate that the files were recently produced. The files depicted close-up images of the pre-pubescent white female child's nude vagina. Based on my training and experience, I believe that the images depict child pornography (as defined by 18 U.S.C. § 2256). Given that the images contained the current date and the undercover officer's name, I believe that the images were produced on November 24, 2015.
  - e. The reset1800@gmail.com account user requested photographs of UCO-1's daughter on a number of occasions, often telling UCO-1 "s2r". The reset1800@gmail.com account user specifically requested nude photographs of UCO's daughter. For example, he stated: "To get mine i'm going to need some nudes :) All mine are!" The reset1800@gmail.com account user later again asked UCO-1: "can u get me full nudes kinda like i got u?". Based on my training and experience, I believe that the reset1800@gmail.com account user was attempting to obtain child pornography from UCO-1.
  - f. Also in the messages exchanged with UCO-1, the reset1800@gmail.com account user discussed on several occasions efforts he took to conceal his identity. The reset1800@gmail.com account user stated that he utilized multiple email accounts as well as an "IP bouncer" to conceal his identity. When UCO-1 suggested that they chat via Kik (a cellular telephone based social media application), the reset1800@gmail.com account user responded: "not really i just don't trust anything that uses a cell phone. ALL CELL PHONES CAN BE TRACED! They can pull your text messages and calls also so they can intercept your images sent through kik that's why i don't use it. Even though it's kik it still uses a cell transmission or data connection to send and rec."
21. On November 27, 2015, the reset1800@gmail.com account user stated that he was changing his email account for "security reasons". He then exchanged emails with UCO-1 from the account child1st@yandex.com. In the exchange of messages, the child1st@yandex.com account user sent UCO-1 an email stating: "here's a link for you. Please view it quick. I'll have to destroy the images in the file so :/ gotta keep the gf happy". The email contained a link to the Yandex file sharing website that contained approximately 14 image files. The child1st@yahndex.com account user told UCO-1 that the files were "recent". Based on my training and experience, I believe that all of the files depict child pornography (as defined by 18 U.S.C. § 2256). The images in summary depicted the following:



- a. A pre-pubescent white female child who is completely naked and captured from the torso down sitting on top of a naked adult white male (whose face is not captured).
  - b. What appears to be a child's hand touching an adult white male's penis.
  - c. What appears to be a white female child performing oral sex on an adult male's penis.
  - d. An adult white male's penis resting on or inserted into the vagina of a pre-pubescent white female child.
  - e. An adult white male secreting semen onto the vagina of a pre-pubescent white female child.
  - f. A pre-pubescent white female child spreading apart her vagina with her hands.
  - g. A blue couch and a bed with grey bedding were captured in the background of two of the images. The adult male was wearing a grey shirt in one of the images.
22. EXIF<sup>1</sup> data was available for approximately 26 of the images that the reset1800@gmail.com account user sent to UCO-1. The EXIF data identified that the images were produced using a Fuji FinePix S8200 camera. EXIF data also identified that all of the images were created in January 2013. Based on my training and experience, I know that account creation date produced in EXIF data can be inaccurate if the date and time settings on the camera are inaccurate, including if the settings are intentionally or unintentionally manipulated by the user. I also know that for some makes and models of cameras, date and time settings can be automatically reset when the batteries are removed from them.
  23. Administrative subpoenas were served to Google requesting subscriber information and logs of IP addresses utilized to log into the account from the time period of November 1, 2015 to November 27, 2015 for the reset1800@gmail.com account. Records received by Google in response to the subpoena identified that the account was created on or about July 15, 2015, in the name of "afav bsdgafe". Based on my training and experience, I know that individuals involved in criminal activities often establish email, telephone, and other accounts in fictitious names in order to conceal their identities from law enforcement. The recovery<sup>2</sup> email account identified for this account was rubmewrong18@hotmail.com. The log of IP addresses identified that the IP address of 174.101.208.24 was utilized on approximately 31 occasions to log into the account. A number of other IP addresses that appeared to be dynamic addresses were utilized on a number of occasions as well.
  24. Records were requested from Time Warner Cable for subscriber information for the IP address of 174.101.208.24. Records from Time Warner Cable identified that the IP address was subscribed to in the name of The Wood Shop at 412 North Main Street, Suite 6, New Carlisle, Ohio (located in Clark County in the Southern District of Ohio); and with a contact telephone number of 937-679-5200. Records were also obtained from Time Warner Cable for a sample of the dynamic IP addresses that were utilized to log

---

<sup>1</sup> EXIF is a format that is a standard for storing interchange information in digital photography image files using JPEG compression. Most new digital cameras use the EXIF annotation, storing information on the image such as shutter speed, exposure compensation, F number, metering system used, if a flash was used, ISO number, date and time the image was taken, etc.

<sup>2</sup> A recovery email account is an alternate email account that a user can establish that Microsoft can send the user's password to in the event that the user forgets his/her password.

- into the account on four separate dates in November 2015, most recently on November 27, 2015. Records from Time Warner Cable identified that each of these IP addresses was assigned to an account that was subscribed to in the name of JAMES RISNER, with a subscriber address of 217 Prentice Drive in New Carlisle, Ohio (also located in Clark County in the Southern District of Ohio) and contact telephone numbers of 937-679-5200 and 937-679-5326.
25. Internet searches for telephone number 937-679-5200 identified that the number was utilized by the business Rescue 1 Custom Vinyls, located at 412 North Main Street, Suite 5, New Carlisle, Ohio. The searches located a number of postings in which an adult female identified as Melissa Risner made comments about this business on the Facebook<sup>3</sup> website. In some of the postings, Melissa Risner identified that the business was owned by her husband, who was a firefighter. For example, on or about June 7, 2015, Melissa Risner posted the following message on a Facebook account in the name "Key West Fire Station 1": "Hi, my husband is a firefighter in midway, ohio. Hehas opened a store in new Carlisle ohio and it is called rescue 1 custom vinyls. He is hoping to have a patch wall from fire departments all over the world. If you can halp me surprise him, by flooding his mailbox with patches that would be AMAZING!! His address is 412 N. Main Street, Suite 5, new Carlisle oh 45344 Thank you and god bless!!"
  26. I have reviewed the property located at 412 North Main Street in New Carlisle, Ohio. I noted that the business contains seven business suites. Each suite has a glass storefront, allowing individuals to see inside the businesses. Written on the glass storefront of Suite 5 was the business name "Rescue 1" and the telephone number "679-5200". There were also writings on the glass indicating that the store sold window decals, vehicle decals, wall decals, vehicle wraps, banners, yard signs, and t-shirts. Seen in plain view inside Suite 5 was a computer monitor that appeared to be connected to a desktop computer tower. Suite 6 did not have any business names posted on its glass or door. However, there was a sign on the door for Suite 6 stating that the door was to be utilized only by Rescue 1 employees. There were also shirts hanging in the window that appeared to be merchandise for the Rescue 1 business. Seen in plain view inside the businesses was an interior open doorway that connected Suite 5 and Suite 6. Based on this information, I believe that Suite 5 and Suite 6 are both utilized by Rescue 1 Custom Vinyls.
  27. Review of Melissa Risner's personal Facebook account as well as various other records checks indicate that Melissa Risner is married to JAMES RISNER. Review of JAMES RISNER's personal Facebook account indicates that he is employed as a firefighter. Review of postings on the Angie's List<sup>4</sup> website identified that the contact person for the Rescue 1 Custom Vinyls business was "Jim Risner".
  28. As noted above, one of the of the photographs in the "gymnastics daughter" album depicted an adult white male, although his face was only captured from the nose down. Based on review of JAMES RISNER's driver's license photograph and photographs on his personal Facebook account, he strongly resembles the male in the photographs.

---

<sup>3</sup> The Facebook website (located at [www.facebook.com](http://www.facebook.com)) is a U.S.-based an online social networking website. Among other features, the website allows users to post pictures, videos, and comments and their accounts and communicate with others via a messenger application.

<sup>4</sup> The Angie's List website (located at [www.angieslist.com](http://www.angieslist.com)) is a U.S.-based paid subscription website containing reviews of local businesses.



29. Photographs and the name of a young female child with blonde hair appeared on Melissa Risner's personal Facebook page. This child will be referred to for purposes of this Affidavit as "Minor Female A". Although she appeared older, Minor Female A resembled the child in the photographs in the "gymnastics daughter" album contained on Website A. As noted above, the reset1800@gmail.com account user identified that his daughter was five years old in these photographs but was currently seven years old. Records from the school that Minor Female A attends identified that she was seven years old, that Melissa Risner was her mother, and that she resided at 217 Prentice Drive in New Carlisle, Ohio. Because Minor Female A has a last name that appears to be Melissa Risner's maiden name or former last name, it is possible that Minor Female A is JAMES RISNER's step-daughter.
30. Based on records from the Ohio Bureau of Motor Vehicles, both JAMES RISNER and Melissa Risner utilize the address of 8945 East State Route 40 in New Carlisle, Ohio, on their current Ohio driver's licenses. Records from the Ohio Bureau of Motor Vehicles identified that JAMES RISNER and Melissa Risner have a 2005 Lincoln Navigator that is jointly registered to them. Although the address used on the registration paperwork was previously the 8945 East State Route 40 address, it was changed to 217 Prentice Drive in New Carlisle, Ohio in July 2015. However, this vehicle has been observed at the 8945 East State Route 40 address on a number of occasions during the time period of November 24, 2015 to November 27, 2015.
31. On November 27, 2015, a deputy of the Clark County Sheriff's Office went to 217 Prentice Drive in New Carlisle, Ohio to make a ruse contact with the occupants. Both JAMES RISNER and Melissa Risner were present at the house. JAMES RISNER confirmed that he owned Rescue 1 Custom Vinyls and would be at the business on the following Monday morning.
32. On November 28, 2015, federal search warrants were authorized by the United States District Court for the Southern District of Ohio for (1) the residential property located at 217 Prentice Drive, New Carlisle, Ohio, 45344, and (2) the business property located at 412 North Main Street, Suites 5 and 6, New Carlisle, Ohio, 45344. Agents and officers of the FBI and Clark County Sheriff's Office executed the warrants on November 29, 2015. Among other items, the following were seized:
  - a. Numerous desktop computers, laptop computers, and other electronic devices (seized from the residence and business);
  - b. Black Fuji FinePix S8200 camera, having a date set to January 1, 2013 (seized from the residence);
  - c. A toilet plunger with a wooden handle (seized from the business);
33. JAMES RISNER was contacted and interviewed during the execution of the search warrants. After being advised of his Miranda Rights, JAMES RISNER provided the following information:

- a. JAMES RISNER lived at 217 Prentice Drive along with his wife, Melissa Risner; his step-daughter, Minor Female A; and his five-year old son. They had resided at the residence since approximately June 2015. An adult male who will be referred to for purposes of this Affidavit as Adult Male A also previously lived at the residence from approximately June 2015 to November 25, 2015. Adult Male A was arrested on November 25, 2015, and has been in the custody of the Clark County Jail since that time.
  - b. JAMES RISNER was the owner of Rescue One Custom Vinyls. Both he and Melissa Risner regularly worked at the business. Adult Male A also worked at the business on a regular basis prior to his arrest.
  - c. JAMES RISNER and Melissa Risner received wireless Internet service through Time Warner Cable at both their residence and business. A password was required to access both accounts. Adult Male A as well as other friends knew the password for the accounts. JAMES RISNER was not aware of anyone other than Melissa Risner and himself using his Internet service since the time of Adult Male A's arrest.
  - d. JAMES RISNER was shown two of the photographs from the "gymnastics daughter" album on Website A. JAMES RISNER identified that Minor Female A was depicted in both of the photographs, and that he was depicted in one of the photographs (the photograph of the adult white male wearing a Cincinnati Bengals shirt). JAMES RISNER stated that he had taken one of the photographs, and Melissa Risner had taken the other photograph. Minor Female A was approximately five years old at the time the photographs were taken. JAMES RISNER claimed that he had posted these and other similar photographs on the Facebook website at one time.
  - e. JAMES RISNER advised that he and Melissa Risner had a black camera, the make and model of which he could not specifically recall. While Melissa Risner sometimes used it, JAMES RISNER was the primary user of the camera. He had taken pictures of Minor Female A with this camera on previous occasions. He typically uploaded the pictures from the camera onto a drive on his laptop computer.
  - f. JAMES RISNER identified that he utilized the email address j.risner@live.com.
  - g. JAMES RISNER denied any utilization of the email accounts reset1800@gmail.com or child1st@yandex.com. He also denied sending any pictures of Minor Female A to anyone via email. Shortly after being asked about the email accounts, JAMES RISNER terminated the interview.
34. Based on records from the Clark County Jail, I confirmed that Adult Male A has been incarcerated since November 25, 2015. As noted above, UCO-1 received email messages from the reset1800@gmail.com and child1st@yandex.com accounts after this date (specifically, on November 26, 2015 and November 27, 2015).
35. Melissa Risner was also interviewed during the execution of the search warrants. I only participated in a small portion of the interview and have not had an opportunity to review a written report or audio recording of the interview at this time. Based on information verbally provided to me by one of the interviewing agents, below is a summary of significant information provided by Melissa Risner:



- a. Melissa Risner reported information that was consistent with that provided by JAMES RISNER about the living arrangements and operation of the business.
  - b. Melissa Risner has never used or heard of the email addresses reset1800@gmail.com or child1st@yandex.com.
  - c. Melissa Risner was shown a sample of photographs that were sent to UCO-1 from the reset1800@gmail.com and child1st@yandex.com accounts. Melissa Risner provided the following information about these photographs:
    - i. Melissa Risner identified Minor Female A as being the individual in approximately six of the photographs based on the child's body parts, clothing, nail polish, scar, and/or other means. These photographs included one of the images that depicted a pre-pubescent white female child with a piece of paper in her hand with UCO-1's undercover name and the date of the email message (November 24, 2015). Melissa Risner recognized this photograph as being taken in the bathroom of the Rescue One Custom Vinyls business. Among other items, Melissa Risner recognized a wooden handle in the background of the image as being a plunger in the bathroom of the business. This handle is consistent with the plunger that was seized from the bathroom of the business during the execution of the search warrant (as detailed above).
    - ii. Melissa Risner recognized the clothing worn by the adult male in approximately two of the photographs to be JAMES RISNER's clothing.
    - iii. Melissa Risner recognized the furniture in approximately two of the photographs to be furniture in her residence.
36. On November 29, 2015 and December 1, 2015, Minor Female A was interviewed by an individual who was trained in conducting forensic interviews of children. In summary, Minor Female A provided the following information during the two interviews:
- a. Minor Female A identified that her father (JAMES RISNER) had taken photographs of what she referred to as her "cookie" (which she identified via an anatomical drawing as a vagina) on a number of occasions. On some occasions, he gave her notes to hold in her hand. These notes contained the names of the individuals to whom he was sending the pictures. On other occasions, JAMES RISNER told Minor Female A to put her finger inside her "cookie" and hold a note while he took the pictures. JAMES RISNER also took pictures of Minor Female A in her underwear and while she was performing gymnastics.
  - b. During the first interview, Minor Female A indicated that she had touched JAMES RISNER's penis with her hand but denied other types of sexual contact. During the second interview, Minor Female A disclosed that JAMES RISNER had vaginal and anal sexual intercourse with her, digitally penetrated her vagina, and performed oral sex on her. He also had her touch his penis and perform oral sex on his penis. These activities often happened at night after he woke her up from sleeping. JAMES RISNER had taken pictures and at least one video of some of these sexual activities.

- c. The first occasion that JAMES RISNER had vaginal sexual intercourse with Minor Female A occurred when she was seven years old. This incident caused a significant amount of bleeding. JAMES RISNER instructed Minor Female A to say that the bleeding was the result of her putting her own fingers inside of her vagina. Minor Female A believed that all of the photographs were taken when she was seven years old.
- d. Some of the photographs were taken at the Rescue 1 business, either in the bathroom or at JAMES RISNER's desk. Although she denied that pictures were taken at her residence during the first interview, Minor Female A identified in the second interview that a number of the pictures were also taken at her residence, including in her bedroom.
- e. JAMES RISNER sent the pictures that he took of Minor Female A to others on the Internet, and these people sent JAMES RISNER pictures of what they did with their daughters.
- f. The camera that JAMES RISNER used to take the pictures of Minor Female A had an "SD chip" in it. He downloaded the pictures onto his computer so that her mother would not find them.
- g. JAMES RISNER showed Minor Female A child pornography on a number of occasions on two websites – Yandex and Website A. Minor Female A stated that JAMES RISNER's password on the Yandex website was "child1st". She also stated that JAMES RISNER had two email accounts that involved the phrase "child1st" – one that was a Google account and one that was a Yandex account.
- h. During the two interviews, Minor Female A was shown a sample of photographs that were sent to UCO-1 from the reset1800@gmail.com and child1st@yandex.com accounts. Although she denied that she was the individual in some of the photographs during the first interview, Minor Female A positively identified herself as being the individual in approximately nineteen of the photographs during the second interview. Minor Female A identified that the photographs were taken at her residence or at the Rescue 1 business. These photographs included the following:
  - i. Images of Minor Female A in her underwear;
  - ii. Close-up images of Minor Female A's vagina and/or buttocks;
  - iii. An image of Minor Female A with a piece of paper in her hand with UCO-1's undercover name and the date of the email message (November 24, 2015);
  - iv. An image of Minor Female A holding a card with "Chillouet 99" written on it and touching her vagina;
  - v. Images of Minor Female A performing oral sex on JAMES RISNER's penis;
  - vi. Images of Minor Female A touching JAMES RISNER's penis;
  - vii. An image of JAMES RISNER secreting semen on Minor Female A's vagina;
  - viii. Images of JAMES RISNER engaging in vaginal sexual intercourse with JAMES RISNER.
- i. JAMES RISNER told Minor Female A not to tell anyone about their sexual activities. JAMES RISNER told her that if she told anyone, he would go to jail for the rest of his life.



- j. At the beginning of the second interview (prior to being shown the photographs), Minor Female A provided the interviewer with a crumpled orange post-it note. Minor Female A identified that this post-it note contained the names of individuals to whom JAMES RISNER sent photographs of her. Minor Female A stated that she found this note on her father's desk earlier that morning. One of the names written on the paper was "Chillouet 99".
37. During a follow-up interview, Melissa Risner identified that Minor Female A had disclosed to her that JAMES RISNER hit her when she did not comply with the sexual activities. Melissa Risner also confirmed that there was an instance in which she found that Minor Female A was bleeding from her vagina, and that Minor Female A said that this was the result of touching her own vagina. Melissa Risner identified that this occurred in July 2015, shortly after Minor Female A's birthday party.
38. Based on my training and experience, I know that victims of child exploitation often do not fully disclose the extent of their sexual abuse during their first or subsequent interviews. Victims may not fully disclose the abuse due to feelings of embarrassment, feelings of affection toward their abusers, or threats made by their abusers, among other reasons. Also in my experience, I know that victims of child pornography offenses sometimes cannot or do not identify themselves in the photographs. Victims may not recognize or want to identify themselves due to feelings embarrassment, their lack of knowledge that the photographs were taken, or the limited focus of the images, among other reasons.
39. A preliminary examination has been conducted at this time of the SD card<sup>5</sup> contained in the Fuji FinePix S8200 camera that was seized from JAMES RISNER's residence pursuant to the search warrant. Recovered on the deleted space of this SD card were six of the images that were sent to UCO-1 on November 27, 2015. Minor Female A also identified that she was the individual depicted in each of the iamges. The images depicted Minor Female A performing oral sex on JAMES RISNER, JAMES RISNER engaging in vaginal sexual intercourse with Minor Female A, and JAMES RISNER secreting semen on Minor Female A's vagina.
40. In reviewing the exterior of the Fuji FinePix S8200 camera, I noted that markings on the bottom of it identified that it was made in China. I therefore submit that the camera affects interstate or foreign commerce.
41. Based on all of the information noted above, I submit that there is probable cause to believe that JAMES RISNER is the user of the [reset1800@gmail.com](mailto:reset1800@gmail.com), [child1st@yandex.com](mailto:child1st@yandex.com), [rubmewrong18@hotmail.com](mailto:rubmewrong18@hotmail.com), and [j.risner@live.com](mailto:j.risner@live.com) accounts. Furthermore, I submit that there is probable cause to believe that JAMES RISNER has produced, distributed, received, and possessed child pornography.

---

<sup>5</sup> A Secure Digital card, commonly referred to as an SD card, is a type of memory card. It is often used to store images or data in digital cameras.

Seizure of the Devices

42. On November 30, 2015, I was contacted by Melissa Risner. Melissa Risner told me that following the execution of the search warrants, she located **Subject Devices** on the floor of her bedroom near a plastic tote. She did not specifically recognize these SD cards. Melissa Risner voluntarily turned over the **Subject Devices** to me and provided her consent for officers to examine them.
43. Based on my training and experience, I know that SD cards are commonly used in digital cameras to store pictures. I know that SD cards are commonly used to store images and other data from digital cameras. I also know that computer files and data can be stored on SD cards when they are plugged into computers through a card reader. Based on all of the information noted in the Affidavit, I believe that JAMES RISNER may have used the **Subject Devices** to store child pornography.
44. The **Subject Devices** are currently stored at the Federal Bureau of Investigation. While the Federal Bureau of Investigation may have all necessary authority to examine the **Subject Devices** based on the previous search warrant and Melissa Risner's consent, I seek this additional warrant out of an abundance of caution to be certain that an examination of the **Subject Devices** will comply with the Fourth Amendment and other applicable laws.

CONCLUSION

45. Based on the aforementioned factual information, I respectfully submit that there is probable cause to believe that evidence, fruits, and instrumentalities of the following criminal offenses may be located on the devices described in Attachment A: (1) possession of child pornography and access with intent to view child pornography, in violation of 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2) and 2252(a)(4)(B); (2) receipt and distribution of child pornography, in violation of 18 U.S.C. §§ 2252A(a)(2)(A) and (b)(1) and 2252(a)(2)(B); (3) production of child pornography, in violation of 18 U.S.C. §§ 2251(a) and (e); and (4) coercion and enticement, in violation of 18 U.S.C. §2422.
46. I, therefore, respectfully request that attached warrants be issued authorizing the search and seizure of the items listed in Attachment B.

//

//

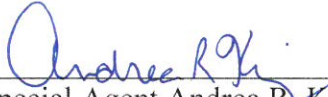
//

//

//



47. Because the warrants for the **Subject Devices** are already in the possession of the Federal Bureau of Investigation, reasonable cause exists to permit the execution of the requested warrants at any time in the day or night.

  
Special Agent Andrea R. Kinzig  
Federal Bureau of Investigation

SUBSCRIBED and SWORN  
before me this 3rd of December 2015

  
Michael J. Newman  
UNITED STATES MAGISTRATE JUDGE

